אלגברה לינארית לחשמל · 05091724

שבוע 1

מבוא - קבוצות, לוגיקה, אינדוקציה, שדות

יוחאי מעין

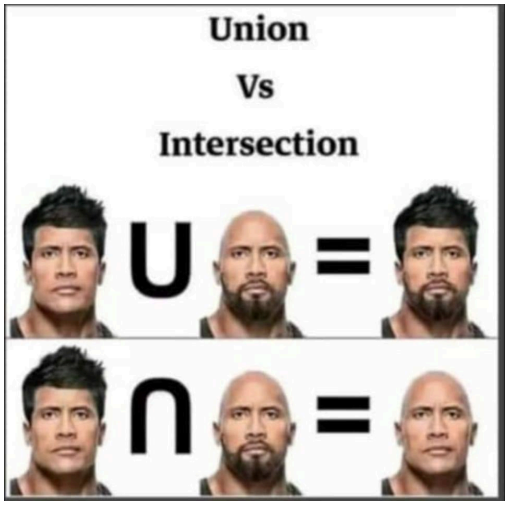
הערות

- המסמך הזה מכיל הערכה לא סופית ולא מחייבת של החומר שיועבר בהרצאות.
- יתכנו חוסרים, שגיאות וכל מיני אי התאמות אחרות ביחס למה שיועבר בפועל.
- הוכחות ינתנו בהרצאות. יש להכיר ולהבין אותן. פירוט נוסף בדוגמאות ובכלל ינתן בהרצאות.
- החומר המחייב הוא החומר אשר מועבר בהרצאות בפועל.
- דיווחים על טעויות במייל yohaim@tauex.tau.ac.il יעזרו מאוד ויתקבלו בשמחה.

תוכן העניינים

1 תורת הקבוצות, לוגיקה, הוכחות, אינדוקציה, הבינום של ניוטון 2
1.1 תורת הקבוצות 2
1.2 לוגיקה 6
1.3 אינדוקציה והבינום של ניוטון 11

2 שדות 15
2.1 הגדרה של שדה 15



1 תורת הקבוצות, לוגיקה, הוכחות, אינדוקציה, הבינום של ניוטון

1.1 תורת הקבוצות

קבוצות

קבוצה במתמטיקה יכולה להתייחס לקבוצה של מספרים כמו $A = \{1, 2, 6\}$ או לקבוצות של אובייקטים מורכבים יותר. כמעט כל אובייקט מתמטי יכול להיות שייך ל / איבר של קבוצה.

יש מספר דרכים לתאר קבוצה: אפשר לפרט מהם איברי הקבוצה (לעיתים ברמיזה, במיוחד אם הקבוצה **אינסופית**); אפשר לתאר מילולית את איברי הקבוצה; ואפשר לתאר קבוצה בתור תת קבוצה של קבוצה אחרת, על ידי ציון תנאי השתייכות.

דוגמאות:

1. הקבוצה $\{1, 2, 6\}$ שראינו קודם מתוארת על ידי פירוט מלא של איבריה. יש בה 3 איברים. למשל, המספר 4 אינו שייך אליה, והמספר 2 שייך אליה.
2. הקבוצה $\{1, 2, \ldots, 10\}$ מפורטת ברמיזה. המספר 7 שייך אליה, והמספר 11 אינו שייך אליה. יש בה 10 מספרים.
3. יש להימנע מתיאור ברמיזה אם עלולה להיות אי הבנה לגבי השתייכות לקבוצה. למשל, האם 6 שייך לקבוצה $\{2, 4, \ldots\}$?
   אם מדובר בקבוצת המספרים הזוגיים החיוביים אז כן. אבל יתכן שהכוונה לקבוצת החזקות של 2, כלומר $\{2, 4, 8, 16, \ldots\}$ ואז לא. במקרה כזה תיאור מילולי יהיה מוצלח יותר: למשל, קבוצת כל המספרים הזוגיים החיוביים.
4. קבוצת הצבעים של דגל ישראל, כלומר $\{\text{לבן}, \text{כחול}\}$.
5. **הקבוצה הריקה** שמסומנת $\emptyset$ היא גם קבוצה; היא פשוט ריקה. אין בה איברים.
6. איברי קבוצה יכולים להיות בעצמם קבוצות. למשל, $C = \{\{1, 2, 6\}, \{1, 3\}\}$ היא קבוצה שיש בה 2 איברים.
   קל להתבלבל - האם $\{2, 6\}$ שייכת לקבוצה C?
   התשובה היא לא. היא לא אחד מהאיברים. היא **מוכלת** באחד מאיברי הקבוצה, ועל כך נדבר מיד.
7. דרך נוספת לתאר קבוצה היא באמצעות תנאי שייכות. למשל, אם נסכים זמנית שהעולם שלנו הוא המספרים על הציר הממשי בלבד,
   $$A = \{x \mid x > 0\}.$$
   יש לקרוא את הקו האנכי | במילים "כך ש-". כלומר, מדובר בקבוצת כל המספרים החיוביים.

חשוב לזכור שבקבוצה אין אפשרות לכפילות ואין חשיבות לסדר. כל הקבוצות הבאות זהות לחלוטין:

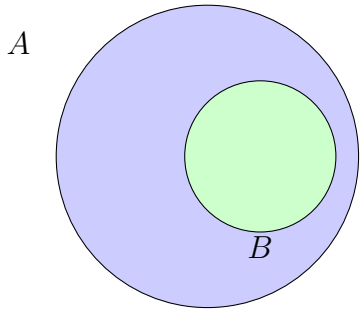
$$\{1, 2, 6\},\ \{2, 1, 6\},\ \{1, 2, 1, 6\},\ \{6, 6, 2, 1, 2, 1, 6, 1, 2, 1, 6\}.$$

הגדרה 1. נסמן $a \in A$ כאשר a שייך לקבוצה A (או: a איבר של הקבוצה A), ואחרת נסמן $a \notin A$.

דוגמה: למשל, $1 \in \{1,2,6\}$ ומצד שני $10 \notin \{1,2,6\}$.

תתי קבוצות

הגדרה 2. תהיינה A, B שתי קבוצות. נאמר שהקבוצה B **מוכלת** בקבוצה A ונסמן $B \subset A$ אם כל איבר של B הוא גם איבר של A, כלומר לכל $b \in B$ מתקיים כי $b \in A$.



הערה: נשתמש גם בסימון $B \subseteq A$, שפירושו זהה לסימון $B \subset A$. בפרט, בשני המקרים יתכן כי $B = A$.

דוגמאות:

1. מתקיים כי $\{1,2\} \subset \{1,2,6\}$. במקרים כאלה לעיתים מסמנים $\{1,2\} \subsetneq \{1,2,6\}$ כי הקבוצות אינן שוות; לרוב לא נשתמש בסימון הזה אלא נסתפק בהכלה "חלשה" שמאפשרת אולי שוויון.
2. הקבוצה $\{1,3\}$ אינה מוכלת בקבוצה $\{1,2,6\}$. אפשר לכתוב $\{1,3\} \not\subset \{1,2,6\}$.
3. לכל קבוצה A מתקיים כי $A \subset A$.
4. אם נתונה $A = \{1,2,6\}$ אז אפשר להגדיר קבוצה B בתור תת קבוצה של A בעזרת תנאי. למשל,

$$B = \{a \in A \mid a \text{ זוגי}\}.$$

כלומר, $B = \{2,6\}$. משמעות הקו $\mid$ היא "כך ש-".

5. הקבוצה $F = \{\{1,2,6\}, \{2,6\}\}$ היא קבוצה שאיבריה הם קבוצות בעצמם. בסימונים של הדוגמה הקודמת, A שייכת לקבוצה זו וכך גם B.
האם הקבוצה $\{1,2\}$ שייכת ל-F?
6. נסמן $A = \{1,2\}$ וכן $B = \{\{1,2\}, \{1,3\}\}$. אז $A \not\subset B$, אבל $A \in B$.

הסימון $B \subseteq A$ זהה לסימון $B \subset A$ מבחינתנו. לעיתים מאמצים מוסכמה אחרת לפיה $\subset$ ו-$\subsetneq$ בעלי משמעות זהה.

קבוצת החזקה

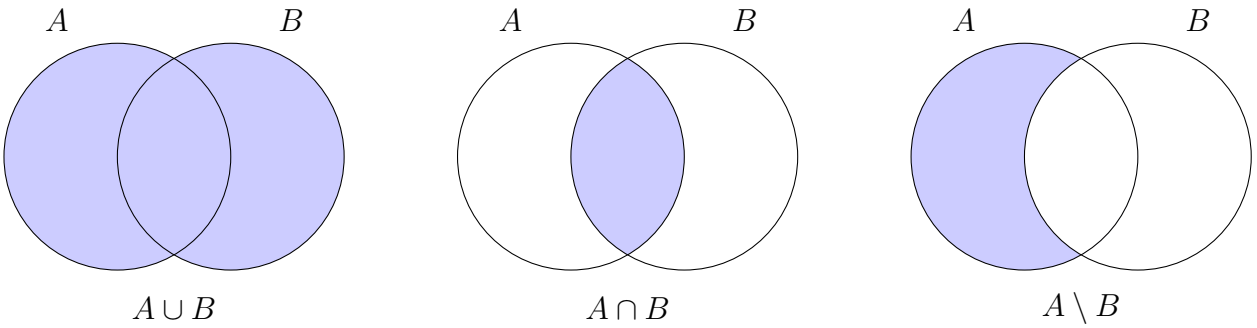
הגדרה 3. תהי A קבוצה. **קבוצת החזקה** של A היא קבוצת כל תתי הקבוצות של A. היא מסומנת $\mathcal{P}(A)$.

דוגמה: קבוצת החזקה של $A=\{1,2,6\}$ היא

$$\mathcal{P}(A)=\{\emptyset,\{1\},\{2\},\{6\},\{1,2\},\{1,6\},\{2,6\},\{1,2,6\}\}.$$

פעולות על קבוצות

הגדרה 4. תהיינה A,B קבוצות.
1. **האיחוד** של A,B הוא הקבוצה $A\cup B=\{c \mid c\in A \text{ או } c\in B\}$.
2. **החיתוך** של A,B הוא הקבוצה $A\cap B=\{c \mid c\in A \text{ וגם } c\in B\}$.
3. **ההפרש** בין A לבין B הוא הקבוצה $A\backslash B=\{c \mid c\in A \text{ וגם } c\notin B\}$.



דוגמאות:
1. נתונות הקבוצות $A=\{1,2,6\}$ ו-$B=\{1,3\}$. אז:

$$A\cup B=\{1,2,3,6\},\ A\cap B=\{1\},\ A\backslash B=\{2,6\},\ B\backslash A=\{3\}.$$

נעיר שקבוצה שיש בה איבר אחד בדיוק מכונה **יחידון**.

2. נתונות הקבוצות $A=\{\{1,2,6\},\{1,7\}\}$ ו-$B=\{\{1,3\},\{7\}\}$. מהו החיתוך $A\cap B$?
איברי הקבוצות הם בעצמם קבוצות. השאלה היא: אילו קבוצות רשומות גם ב-A וגם ב-B. התשובה לכך היא: אף קבוצה. לכן $A\cap B=\emptyset$. במקרה כזה אומרים כי A,B קבוצות **זרות**.
זה לפעמים מבלבל ונוטים לחשוב שהקבוצה $\{1\}$ למשל שייכת לחיתוך. אבל היא לא ב-A ולא ב-B! האיברים הם קבוצות; לא חותכים בין האיברים.

לעיתים מוסכם שעובדים רק עם תתי קבוצות של קבוצה מסוימת ברורה A. במקרה זה, **המשלים** של קבוצה B (שהיא לכן תת קבוצה של A) הוא ההפרש $A\backslash B$. מסמנים את המשלים של B על ידי B^c.

דוגמה: בכיתה א' יש רק מספרים שלמים אי שליליים. לכן כל קבוצה (זוגיים, אי זוגיים) היא תת קבוצה של קבוצה זו:

$$A = \{0, 1, 2, \ldots\}.$$

בהקשר זה מתקיים למשל כי $\{1, 2, 3, \ldots\}^c = \{0\}$.

הערה: יש סימון מקובל אחר למשלים, שאנחנו לא נשתמש בו: $\overline{B}$.

אם זה לא ברור לגמרי מי הקבוצה הגדולה A אז עדיף לא להשתמש במושג המשלים אלא לכתוב במפורש $A\backslash B$.

קבוצות של מספרים

המספרים הממשיים, בשונה מקבוצות מספרים פשוטות יותר שנזכיר מיד, הם חמקמקים. כולם מכירים את המספר π, שהוא דוגמה מצוינת למספר ממשי. אבל מה התיאור של "המספרים הממשיים"? כדי להבין את כוונת השאלה, הנה כמה קבוצות מספרים חשובות לפי סדר היסטורי:

שם	סימון	תיאור	הערות
המספרים הטבעיים	$\mathbb{N}$	המספרים $1, 2, 3, \ldots$	בסיסיים ביותר, משמשים לספירה.
המספרים השלמים	$\mathbb{Z}$	הטבעיים, בתוספת 0 והשלמים השליליים: $\ldots, -3, -2, -1, 0, 1, 2, 3 \ldots$	מספרים מתבקשים, כדי לעקוב אחרי חובות למשל.
המספרים הרציונלים	$\mathbb{Q}$	מנות של שלמים: $\frac{m}{n}$, כאשר $m, n \in \mathbb{Z}$ ו-$n \neq 0$	גם אלו מספרים שמתבקש להשתמש בהם. למשל, חצי תפוח. באופן יותר מתמטי, פתרונות למשוואות פשוטות עם מקדמים שלמים: $nx = m$.
המספרים הממשיים	$\mathbb{R}$	כל המספרים שעל הציר	זהו תיאור לא מדויק אבל נסתפק בו.
המספרים המרוכבים	$\mathbb{C}$	המספרים $a + bi$ כאשר $i^2 = -1$ ו-$a, b \in \mathbb{R}$	פירוט ינתן בתרגול.

הערות:

- עבורנו המספר 0 אינו מספר טבעי. כלומר, $0 \notin \mathbb{N}$. לעיתים מסכימים שכן, כלומר אין בעולם מוסכמה מוחלטת.
- המספר הרציונלי $\frac{m}{n}$ כמובן שאינו מוגדר עבור $n = 0$. נעיר גם שזה מספיק לאפשר ל-m להיות שלילי כדי לכסות ממילא את כל התוצאות האפשריות של מנה של שני שלמים. למשל, $\frac{2}{-4} = \frac{-1}{2}$. לכן נהוג לכנות "ייצוג קנוני" (קנוני - שאינו תלוי בבחירה שרירותית) כאשר $m \in \mathbb{Z}$, $n \in \mathbb{N}$ והמספרים m, n זרים. לכל מספר רציונלי יש ייצוג קנוני יחיד.
- אולי $\mathbb{Q}$ זה בכלל כל המספרים שעל הציר (למשל, אולי π רציונלי: שווה למנה של שני שלמים)? במילים אחרות, אולי $\mathbb{R} = \mathbb{Q}$? מתברר שלא. למשל, $\sqrt{2}, \pi, e$ הם דוגמאות של מספרים ממשיים (על הציר) שאינם רציונלים. מספר ממשי שאינו רציונלי מכונה **אי רציונלי**.

שוויון קבוצות

אם נתונות שתי קבוצות A, B ורוצים להוכיח שהן שוות, ברוב המוחלט של המקרים נעשה זאת על ידי **הכלה דו כיוונית**: נוכיח כי $A \subset B$ וגם $B \subset A$.

דוגמה: נסמן $A = \mathbb{Q}$ ונסמן ב-B את קבוצת המספרים x שהם פתרונות של **משוואה לא טריוויאלית ממעלה 1 מעל** $\mathbb{Z}$: $ax + b = 0$ כאשר $a, b \in \mathbb{Z}$. ליתר דיוק,

$$B = \{x \in \mathbb{R} \mid ax + b = 0 \text{ כך ש-}0 \text{ לא שניהם } a, b \in \mathbb{Z} \text{ קיימים}\}.$$

נוכיח כי $A = B$ באמצעות הכלה דו כיוונית.
נוכיח כי $A \subset B$. יהי $x \in A$. לפי ההגדרה, $A = \mathbb{Q}$ ולכן x רציונלי.
לכן קיימים $m, n \in \mathbb{Z}$ (כאשר $n \neq 0$) כך ש-$x = \frac{m}{n}$. לכן $m = nx$ ולכן $nx - m = 0$.
נסמן $a = n,\ b = -m$. אז $a, b \in \mathbb{Z}$ לא שניהם 0 ומתקיים כי $ax + b = 0$. לכן $x \in B$.
הוכחנו שאם $x \in A$ אז $x \in B$ ולכן $A \subset B$.

נוכיח כי $B \subset A$. יהי $x \in B$. לכן לפי ההגדרה קיימים $a, b \in \mathbb{Z}$ לא שניהם 0 כך שמתקיים $ax + b = 0$.
אם $a = 0$ אז $0 \cdot x + b = 0$, כלומר $b = 0$. לכן $a = b = 0$. זה לא יתכן ולכן $a \neq 0$.
לכן $x = \frac{-b}{a}$. המספרים $a, -b$ שלמים ולכן $\frac{-b}{a} \in \mathbb{Q}$. לכן $x \in A$.
הוכחנו שאם $x \in B$ אז $x \in A$ ולכן $B \subset A$.

לסיכום, הוכחנו כי $A \subset B$ וגם $B \subset A$. לכן $A = B$.

1.2 לוגיקה

כמתים ונוסחאות

הסימנים $\forall$ ו-$\exists$ מכונים **כמתים**.

המשמעות של $\forall$ היא **לכל**. למשל, הביטוי: $\forall n \in \mathbb{N}$ הוא "לכל n טבעי".

המשמעות של $\exists$ היא **קיים**. למשל, הביטוי: $\exists n \in \mathbb{N}$ הוא "קיים n טבעי".

בעזרת הכמתים הללו ניתן ליצור **נוסחאות**.

דוגמאות:
1. הפסוק $\forall x \in \mathbb{R}\ x^2 \geq 0$ הוא נכון.
2. הפסוק $\forall x \in \mathbb{C}\ x^2 \geq 0$ אינו נכון כי למשל $(i)^2 = -1 < 0$.

המשמעות של הסימן $\rightarrow$ או $\Rightarrow$ היא **גורר**. לרוב נשתמש ב-$\Rightarrow$.

דוגמאות:
1. נתבונן בנוסחה $\forall x \in \mathbb{R}\,(x < 2 \Rightarrow x^2 < 2)$. האם היא נכונה?
   לא, למשל: $x = -5$.

2. הנה מספר נוסחאות דומות:

נוסחה	נכונות
$\forall x \in \mathbb{R}\ \forall n \in \mathbb{Z}\ x+n>0$	שקר
$\forall n \in \mathbb{Z}\ \forall x \in \mathbb{R}\ x+n>0$	שקר
$\forall x \in \mathbb{R}\ \exists n \in \mathbb{Z}\ x+n>0$	אמת
$\exists n \in \mathbb{Z}\ \forall x \in \mathbb{R}\ x+n>0$	שקר
$\forall n \in \mathbb{Z}\ \exists x \in \mathbb{R}\ x+n>0$	אמת
$\exists x \in \mathbb{R}\ \forall n \in \mathbb{Z}\ x+n>0$	שקר

ניתן להחליף סדר בין שני $\forall$ או שני $\exists$ והמשמעות תישאר זהה (כלומר, יתקבלו נוסחאות שקולות). בדרך כלל אי אפשר להחליף סדר בין $\forall$ לבין $\exists$.

וגם, או

הסימון $\wedge$ פירושו **וגם**.

הסימון $\vee$ פירושו **או**.

הסימנים $\wedge$ ו-$\vee$ מכונים **קשרים לוגיים**.

דוגמה: הנוסחה $\forall x \in \mathbb{R} \exists n \in \mathbb{N}\,([x]=n \wedge n \le x)$ פירושה שלכל x ממשי קיים n טבעי אשר שווה לערך השלם של x וגם קטן או שווה ל-x.
זו נוסחה שקרית. למשל, $x=-1.3$, עבורו $[x]=-2$.
לכן אין אף n **טבעי** עבורו $n=[x]$.

באופן מדויק יותר, לכל נוסחה מיוחסת נכונות: אמת או שקר. הסימונים $\wedge$ ו-$\vee$ מוגדרים דרך **טבלאות האמת** שלהם כדלקמן.

P	Q	$P \wedge Q$	$P \vee Q$
אמת	אמת	אמת	אמת
אמת	שקר	שקר	אמת
שקר	אמת	שקר	אמת
שקר	שקר	שקר	שקר

שלילה

המשמעות של הקשר הלוגי $\neg$ היא **שלילה**.

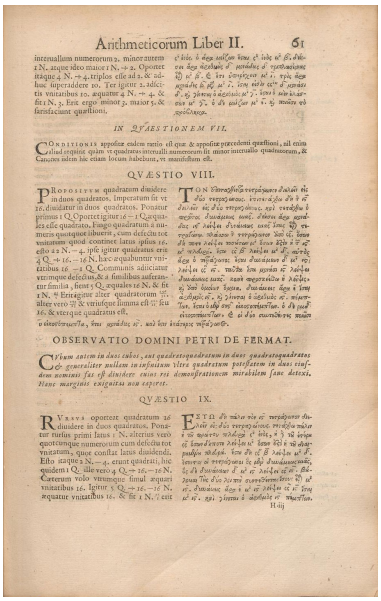
P	$\neg P$
אמת	שקר
שקר	אמת

דוגמאות:
1. הביטוי: $\neg\,(\exists n \in \mathbb{N})$ הוא "לא קיים n טבעי". אין כאן פסוק ולכן אין טעם לשאלה אם נכון או לא.

2. הפסוק $\forall n \in \mathbb{N} \ (n > 2 \Rightarrow \neg (\exists x, y, z \in \mathbb{N} \ x^n + y^n = z^n))$ מכונה **המשפט האחרון של פרמה**.
יש כאן שימוש בכתיב המקוצר $\exists x, y, z \in \mathbb{N}$ שמשמעותו

$$\exists x \in \mathbb{N} \ \exists y \in \mathbb{N} \ \exists z \in \mathbb{N}$$

(לא משנה באיזה סדר, כפי שראינו), כלומר: קיימים x, y, z טבעיים.
מה משמעות הפסוק? אם $n > 2$ טבעי, אז **לא** קיימים x, y, z טבעיים שפותרים את המשוואה $x^n + y^n = z^n$.
בשביל ההקשר, במקרה $n = 2$ המשוואה היא **משוואת פיתגורס** $x^2 + y^2 = z^2$. כידוע, בכל משולש ישר הזווית אורכי הניצבים x, y והיתר z מקיימים משוואה זו. כידוע, יש משולשים ישרי זווית בעלי צלעות עם אורכים שלמים. למשל, $x = 3, y = 4, z = 5$. יש עוד אינסוף כאלה שלשות. הן מכונות **שלשות פיתגוריות**.
פרמה שיער שאין אף פתרון למשוואה $x^3 + y^3 = z^3$ שבו x, y, z טבעיים. הוא הוסיף הערה בעותק שלו של הספר המפורסם Arithmetica: "יש בידי הוכחה באמת מופלאה לזה, ששוליים אלו צרים מכדי להכילה".


Arithmetcorum Liber II. 61

IN QVÆSTIONEM VII.

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

כך גם לכל $n \geq 3$ אחר. מתמטיקאים ניסו והקדישו את חייהם אך לא מצאו הוכחה, עד שבשנת 1994 המתמטיקאי אנדרו ויילס פרסם הוכחה נכונה.
נתבונן בביטוי הפנימי $\neg (\exists x, y, z \in \mathbb{N} \ x^n + y^n = z^n)$. אפשר לכתוב אותו גם אחרת: אם לא קיימים x, y, z טבעיים עבורם יש שוויון, הרי שלכל x, y, z טבעיים אין שוויון. כלומר:

$$\neg (\exists x, y, z \in \mathbb{N} \ x^n + y^n = z^n) \equiv \forall x, y, z \in \mathbb{N} \ x^n + y^n \neq z^n.$$

המשמעות של הסימן $\equiv$ היא **שקול**.
לכן ניתן לכתוב את המשפט האחרון של פרמה גם כך:

$$\forall n \in \mathbb{N} \ (n > 2 \Rightarrow (\forall x, y, z \in \mathbb{N} \ x^n + y^n \neq z^n)).$$

שקילות נוסחאות

באופן כללי, נכתוב $P \equiv Q$ אם P, Q בעלות אותה נכונות (שתיהן שקר, או שתיהן אמת).

באופן מדויק יותר, אם P, Q בנויות מפסוקים בסיסיים שנכונותם אינה ידועה, אז נכתוב $P \equiv Q$ אם ל-P, Q יש אותה טבלת אמת (בהתבסס על הנכונות האפשרית של הפסוקים הבסיסיים שמהם הן בנויות).

עקרונות לשלילה של נוסחה

באופן כללי, ניתן לשלול נוסחה בעזרת העיקרון $\forall \leftrightarrow \exists$. ליתר דיוק:

1. $\neg\left(\forall x P\left(x\right)\right) \equiv \exists x \neg P\left(x\right)$.
2. $\neg\left(\exists x P\left(x\right)\right) \equiv \forall x \neg P\left(x\right)$.
3. $\neg\left(P \Rightarrow Q\right) \equiv P \wedge \neg Q$.
4. $\neg\left(P \wedge Q\right) \equiv \left(\neg P\right) \vee \left(\neg Q\right)$.
5. $\neg\left(P \vee Q\right) \equiv \left(\neg P\right) \wedge \left(\neg Q\right)$.

כדי להבין את העיקרון השלישי (שהוא בדרך כלל המאתגר ביותר להבנה), נכתוב טבלת אמת עבור הנוסחה $P \Rightarrow Q$:

P	Q	$P \Rightarrow Q$
אמת	אמת	אמת
אמת	שקר	שקר
שקר	אמת	אמת
שקר	שקר	אמת

כלומר, המקרה היחיד שבו $P \Rightarrow Q$ לא מתקיים הוא כאשר P אמת וגם Q שקר. במילים אחרות, $P \wedge \neg Q$.

דוגמאות:

1. ראינו שהנוסחה $\exists n \in \mathbb{Z}\ \forall x \in \mathbb{R}\ x + n > 0$ היא שקרית. לכן השלילה שלה תהיה אמת. נקבל את הנוסחה $\forall n \in \mathbb{Z}\ \exists x \in \mathbb{R}\ x + n \leq 0$. ובאמת, לכל n שלם יש x ממשי כך ש-$x + n$ אי חיובי.
2. המשפט האחרון של פרמה: $\forall n \in \mathbb{N}\ \ (n > 2 \Rightarrow (\forall x, y, z \in \mathbb{N}\ x^n + y^n \neq z^n))$. השלילה שלו היא לכן
$$\exists n \in \mathbb{N}\ n > 2 \wedge (\exists x, y, z \in \mathbb{N}\ x^n + y^n = z^n).$$
כלומר, קיים $n > 2$ טבעי עבורו יש פתרון למשוואה $x^n + y^n = z^n$ שמורכב ממספרים טבעיים. כאמור, זה שקר.
3. הנוסחה $P = \forall x \in \mathbb{R} \exists n \in \mathbb{N}\, [x] = n$ שקרית. לכן
$$\neg\left(P\right) = \exists x \in \mathbb{R} \forall n \in \mathbb{N}\, [x] \neq n$$
אמת. פירושה: קיים מספר ממשי x כך שלכל n טבעי מתקיים כי $[x] \neq n$. ואכן, למשל, $x = -1.3$ מקיים $[x] = -2$, ולכל n טבעי מתקיים כי $n \neq -2$.

הוכחה על ידי גרירה הפוכה

עובדה בסיסית חשובה היא שהנוסחה $P \Rightarrow Q$ תמיד שקולה לנוסחה $\neg Q \Rightarrow \neg P$. כלומר,

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P) .$$

נוודא, באמצעות טבלאות אמת:

P	Q	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
אמת	אמת	שקר	שקר	אמת
אמת	שקר	שקר	אמת	שקר
שקר	אמת	אמת	שקר	אמת
שקר	שקר	אמת	אמת	אמת

זו אותה טבלת אמת כמו של $P \Rightarrow Q$, ולכן הן אכן שקולות.

לכן אם הוכחנו $\neg Q \Rightarrow \neg P$, אפשר מיד להסיק $P \Rightarrow Q$.

לפעמים מכנים את $\neg Q \Rightarrow \neg P$ ה**קונטרה-פוזיטיב** של $P \Rightarrow Q$.

דוגמאות:

1. לכל כלב יש 4 רגליים. אם נסמן "אני כלב" ב-P ו"יש לי 4 רגליים" ב-Q, הרי ש-$P \Rightarrow Q$.
לפי העיקרון הנ"ל, זה גם נכון ש-$\neg Q \Rightarrow \neg P$. כלומר: אם אין לי 4 רגליים, אני לא כלב.
חשוב לשים לב שזה שונה מאשר $Q \Rightarrow P$: זה לא נכון שאם **יש** לי 4 רגליים אז אני כלב. למשל, אולי אני חתול.
2. נתונה טענה (כלומר, נוסחה): אם n טבעי ו-p מספר ראשוני (מספר טבעי גדול מ-1 שמתחלק רק בעצמו וב-1) אז $p \mid n^2 \Rightarrow p \mid n$. למשל, אם n^2 מתחלק ב-3 אז גם n בהכרח מתחלק ב-3. או מקרה יותר מוכר: אם n^2 זוגי אז גם n זוגי.
איך נוכיח טענה כזו? במקרים מסוימים, יותר קל להוכיח את הטענה השקולה $\neg Q \Rightarrow \neg P$. ובאמת, במקרה שלנו, יותר קל להוכיח כי $p \nmid n \Rightarrow p \nmid n^2$. כדי לעשות זאת נשתמש במשפט שאולי נוכיח בהמשך: כל מספר טבעי $n > 1$ ניתן לכתיבה באופן יחיד (עד כדי שינוי סדר הגורמים) כמכפלה של מספרים ראשוניים, ורק הראשוניים אשר מופיעים בפירוק מחלקים את המספר n.
נניח כי $p \nmid n$. לפי המשפט ניתן לכתוב $n = q_1 \cdots q_k$ כאשר $q_1, \ldots, q_k$ ראשוניים. לפי ההנחה, p אינו אחד מבין $q_1, \ldots, q_k$.
לכן $n^2 = q_1 q_1 \cdots q_k q_k$. זהו הייצוג של n^2 כמכפלה של מספרים ראשוניים, ו-p אינו בין הגורמים.
לכן $p \nmid n^2$.
בסך הכל הוכחנו כי $p \nmid n \Rightarrow p \nmid n^2$, או באופן שקול $p \mid n^2 \Rightarrow p \mid n$.

באופן כללי, כדי להוכיח $P \Rightarrow Q$, ניתן להוכיח באופן שקול כי $\neg Q \Rightarrow \neg P$. זה לא תמיד כדאי אבל לפעמים כן.

הוכחה בדרך השלילה

שיטת ההוכחה בדרך השלילה היא שיטה חזקה ושימושית מאוד. לעיתים מבלבלים בינה לבין השיטה הקודמת של הוכחת $\neg Q \Rightarrow \neg P$, כאשר למעשה היא מכלילה אותה.

נניח שברצוננו להוכיח כי $P \Rightarrow Q$. שיטת ההוכחה בשלילה היא להניח כי $P \wedge \neg Q$ (כלומר, את שלילת הנוסחה שרוצים להוכיח). קוראים לזה **הנחת השלילה**. אם מכך ניתן להוכיח פסוק שקר, אז הנחת השלילה שגויה. פסוק השקר מכונה **סתירה** ואם שלילת הטענה היא שקר, אז הטענה נכונה.

דוגמה: נוכיח שאם $r \in \mathbb{Q}$ אז $r^2 \neq 2$. כלומר, המספר $\sqrt{2}$ אינו מספר רציונלי.
לפי אגדה אורבנית (וכנראה שקרית), אחד מאנשי פיתגורס ששמו היפסוס (Hippasus) הציג הוכחה לכך שקיים מספר "בעולם האמיתי" שאינו רציונלי. לפי אותו סיפור, הוא עשה זאת לצערו על גבי סירה ובחברת מספיק אנשי פיתגורס (ואולי אף בנוכחות המאסטר בכבודו ובעצמו). הוא מצא את עצמו בדרכו לקרקעית האגם.
נניח בשלילה שקיים מספר רציונלי r כך ש-$r^2 = 2$. אז יש אפשרות לכתוב את $r = \frac{m}{n}$, ייצוג קנוני. נקבל אם כך $\frac{m^2}{n^2} = 2$, כלומר $m^2 = 2n^2$.
זה אומר ש-m^2 מתחלק ב-2, ומכיוון ש-2 ראשוני, גם m מתחלק ב-2. כלומר, אפשר לכתוב $m = 2k$ כאשר k איזשהו מספר שלם. אבל אז נקבל: $2n^2 = m^2 = (2k)^2 = 4k^2$, כלומר, $n^2 = 2k^2$.
לכן n^2 זוגי, וכאמור זה אומר שבעצם n זוגי. לכן m, n שניהם זוגיים. אבל זו סתירה, כי לקחנו $r = \frac{m}{n}$ ייצוג קנוני ובפרט m, n זרים!
לכן אין מספר רציונלי שמקיים $r^2 = 2$.

1.3 אינדוקציה והבינום של ניוטון

עיקרון האינדוקציה והוכחה באינדוקציה

עיקרון האינדוקציה המתמטית הוא פשוט ותמים למראה. נניח כי $A \subset \mathbb{N}$ מקיימת שני תנאים:

1. $1 \in A$.
2. $n \in A \Rightarrow n + 1 \in A$.

אז $A = \mathbb{N}$.

העיקרון הזה הופך לחזק במיוחד כאשר משתמשים בו כיסוד להוכחות. נניח שנתונה **סדרה של טענות** (פסוקים) $P(1), P(2), \ldots$. למשל, הטענה $P(n)$ יכולה להיות: $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. השיטה של **הוכחה באינדוקציה** אומרת שאם:

1. $P(1)$ נכונה (**בסיס האינדוקציה**).
2. $P(n) \Rightarrow P(n+1)$ לכל $n \in \mathbb{N}$ (**צעד האינדוקציה**).

אז לכל $n \in \mathbb{N}$ מתקיים כי $P(n)$ נכונה.

כדי להוכיח באינדוקציה יש לכן שני שלבים: בסיס האינדוקציה שבו מוכיחים כי $P(1)$ נכונה, ואז צעד האינדוקציה שבו מוכיחים כי $P(n) \Rightarrow P(n+1)$. כלומר, כדי להשלים את צעד האינדוקציה, יש להניח כי $P(n)$ נכונה (זה נקרא **הנחת האינדוקציה**) ומכך להוכיח את $P(n+1)$.

דוגמאות:

1. נוכיח באינדוקציה שלכל $n \in \mathbb{N}$ מתקיים כי $1+2+\cdots+n=\frac{n(n+1)}{2}$.
בסיס: עבור $n=1$, $\frac{1\cdot(1+1)}{2}=1$ (אכן יש שוויון).
צעד: עבור $n \in \mathbb{N}$, נניח כי $1+2+\cdots+n=\frac{n(n+1)}{2}$ (זו הנחת האינדוקציה) ונוכיח כי

$$1+2+\cdots+(n+1)=\frac{(n+1)\cdot(n+1+1)}{2}$$

ואכן, בעזרת הנחת האינדוקציה,

$$1+2+\cdots+(n+1)=1+2+\cdots+n+(n+1)=\frac{n\,(n+1)}{2}+n+1$$
$$=\frac{n\,(n+1)+2\,(n+1)}{2}=\frac{(n+1)\,(n+2)}{2}$$

2. סדרה $a_1,a_2,a_3,\ldots$ מכונה **סדרה חשבונית** אם $a_2-a_1=a_3-a_2=\cdots$, כלומר: קיים $d \in \mathbb{R}$ כך שלכל $n \in \mathbb{N}$ מתקיים כי $a_{n+1}=a_n+d$.
נוכיח באינדוקציה שעבור סדרה כזו מתקיים: לכל $n \in \mathbb{N}$, $a_n=a_1+(n-1)\,d$.
בסיס האינדוקציה: אם $n=1$ אז אגף שמאל הוא a_1 ואגף ימין הוא $a_1+(1-1)\cdot d=a_1$. לכן יש שוויון. בכך הוכחנו את נכונות $P(1)$.
צעד האינדוקציה: נניח שידוע כי $a_n=a_1+(n-1)\,d$, כלומר ידוע כי $P(n)$ אמת. נוכיח כי $P(n+1)$ אמת, כלומר: $a_{n+1}=a_1+(n+1-1)\,d=a_1+nd$.
ואכן,

$$a_{n+1}=a_n+d=a_1+(n-1)\,d+d=a_1+nd.$$

לכן סיימנו.

3. נסו לכתוב הוכחה באינדוקציה שאם $a_1,a_2,\ldots$ סדרה הנדסית (כלומר $a_{n+1}=qa_n$ לכל $n \in \mathbb{N}$) אז $a_n=a_1q^{n-1}$.

שימוש בבסיס אינדוקציה מותאם

דוגמה: נוכיח שכל הסוסים בעולם הם באותו צבע.
ליתר דיוק, נוכיח באינדוקציה שלכל n מתקיים שכל n סוסים הם באותו צבע.
בסיס האינדוקציה: עבור $n=1$, ברור שכל n סוסים הם באותו צבע כי מדובר בסוס יחיד. הוא באותו צבע כמו עצמו.
צעד האינדוקציה: נניח שידוע שכל n סוסים הם באותו צבע, ונניח שנתונים $n+1$ סוסים. נוכיח שכל $n+1$ הסוסים הם באותו צבע.
ואכן, n הסוסים הראשונים הם באותו צבע לפי הנחת האינדוקציה. נקרא לצבע הזה X. גם n הסוסים האחרונים (כלומר, כולם חוץ מהראשון). לפי כל הסוסים באמצע, הצבע הזה הוא X. לכן כל $n+1$ הסוסים הם בצבע X ולכן $n+1$ הסוסים הם באותו צבע.

ברור שהטענה שגויה. איפה, אם כך, השקר?

לא כל אינדוקציה חייבת להתחיל מ-$n=1$. אם הבסיס או הצעד אינם נכונים עבור $n=1$ אז כדאי לפעמים לחפש n גדול יותר שהחל ממנו שניהם נכונים.

דוגמאות:

1. נוכיח שלכל $n \geq 3$ מתקיים כי $2n+1 < 2^n$.
בסיס האינדוקציה: עבור $n = 3$ מתקיים כי $2n + 1 = 7 < 8 = 2^n$.
צעד האינדוקציה: יהי $n \geq 3$ ונניח שידוע כי $2n + 1 < 2^n$. נוכיח כי $2(n+1)+1 < 2^{n+1}$.
ואכן, $2(n+1)+1 = 2n+1+2$. לכן לפי הנחת האינדוקציה מתקיים כי

$$2(n+1)+1 < 2^n + 2 < 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

2. נוכיח שלכל $n \geq 5$ מתקיים כי $n^2 < 2^n$.
בסיס האינדוקציה: עבור $n = 5$ מתקיים כי $n^2 = 25 < 32 = 2^n$.
צעד האינדוקציה: יהי $n \geq 5$ ונניח שידוע כי $n^2 < 2^n$. נוכיח כי $(n+1)^2 < 2^{n+1}$.
ואכן, $(n+1)^2 = n^2 + 2n + 1$. לפי הנחת האינדוקציה מתקיים כי $n^2 < 2^n$ ולכן בעזרת הדוגמה הקודמת ($n \geq 5$),

$$(n+1)^2 < 2^n + 2n + 1 < 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

נשים לב שאי השוויון $n^2 < 2^n$ מתקיים עבור $n = 1$ ולכן אפשר היה לחשוב שזה בסיס חוקי. אם זה היה המצב אז אי השוויון היה נכון לכל $n \in \mathbb{N}$, אבל עבור $n = 3$ למשל הוא לא נכון. הבעיה היא בצעד האינדוקציה, אשר שגוי עבור $n = 1$ (ולא רק) כי לא מתקיים $2n + 1 \leq 2^n$.

סימן הסכום

בקורס ובכלל במתמטיקה נפגוש לעיתים קרובות סכומים של מספר משתנה של איברים. במקרים כאלה (ולמעשה לא רק), נוח להשתמש בסימן הסכום $\sum_{k=1}^{n} a_k = a_1 + \cdots + a_n$.

דוגמאות:

1. $\sum_{k=1}^{17} 1 = 1 + 1 + \cdots + 1 = 17$.
2. $\sum_{k=1}^{6} k = 1 + 2 + 3 + 4 + 5 + 6 = 21$.
3. $\sum_{k=1}^{n} k = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. הוכחנו את זה באינדוקציה!
4. מהו $\sum_{k=1}^{n} (-1)^k$?
למשל,

$$\sum_{k=1}^{5} (-1)^k = (-1) + 1 + (-1) + 1 + (-1) = -1.$$

נעיר שאפשר "לשכן" סימני סכום, וניתקל בזה בעתיד. למשל, $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij}$.

הבינום של ניוטון

הנוסחה $(a+b)^2 = a^2 + 2ab + b^2$ היא אחת מבין **נוסחאות כפל מקוצר** אשר מוכרות מהתיכון. היא קלה להוכחה:

$$(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 = a^2 + 2ab + b^2.$$

יש נוסחה גם עבור העלאה בשלישית, גם היא קלה להוכחה: $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

אם נתעלם מהמקדמים $1,2,1$ או $1,3,3,1$, בשני המקרים יש תבנית: סכום של כל המכפלות a^2b^0, a^1b^1, a^0b^2 במקרה הראשון או $a^3b^0, a^2b^1, a^1b^2, a^0b^3$ במקרה השני. כלומר, a^kb^{n-k} עבור $k = 0, \ldots, n$ (n הוא 2 או 3).

מתברר שיש הכללה: נוסחה עבור $(a+b)^n$. במקרה $n = 2, 3$ מקבלים את שתי הנוסחאות הנ"ל. עבור $n = 4$ למשל, נקבל משהו כזה:

$$(a+b)^4 = \underline{?}a^4 + \underline{?}a^3b + \underline{?}a^2b^2 + \underline{?}ab^3 + \underline{?}b^4.$$

בשביל לקבל תחושה, נחזור למקרה $n = 3$. במקום לפתוח ללא מחשבה, נכתוב ראשית

$$(a+b)^3 = (a+b)(a+b)(a+b).$$

התוצאה היא סכום של מחוברים, שכל אחד מהם הוא מכפלה של שלושה גורמים: אחד מכל סוגריים. למשל, אם נבחר a, a, a נקבל $a \cdot a \cdot a = a^3$. אם נבחר a, b, a נקבל a^2b, אבל גם אם נבחר b, a, a או a, a, b. אלו כל האפשרויות לקבלת a^2b ולכן בתוצאה המחובר הזה יופיע 3 פעמים. לכן, $3a^2b$.

במקרה הכללי,

$$(a+b)^n = (a+b)\cdots(a+b).$$

יש n סוגריים זהים. ברור שיש רק דרך אחת לקבל a^n: צריך לבחור a בכל סוגריים. לכן בתוצאה יופיע a^n בדיוק פעם אחת.

מצד שני, כמה דרכים יש לקבל $a^{n-1}b$? יש לבחור זוג סוגריים אחד מבין ה-n ובו לבחור b, ובשאר a. כלומר, יש n אפשרויות. לכן נקבל את המחובר $a^{n-1}b$ בדיוק n פעמים. באופן דומה:

$$(a+b)^n = a^n + na^{n-1}b + \cdots + nab^{n-1} + b^n.$$

מה עם שאר המחוברים? כמה פעמים יופיע המחובר a^kb^{n-k}? יש לבחור k זוגות סוגריים מתוך ה-n ובהם לקחת את a. באחרים, לקחת את b. כמה דרכים יש לבחור k זוגות סוגריים מתוך ה-n? באופן שקול, כמה דרכים יש להרכיב קבוצה של k אנשים מתוך קבוצה נתונה של n אנשים?

מתברר שהתשובה היא $\frac{n!}{k!(n-k)!}$. המספר הזה מסומן $\binom{n}{k}$ ומכונה n **מעל** k או n **בחר** k.

משפט 5. לכל $a, b \in \mathbb{R}$ ו-$n \in \mathbb{N}$ מתקיים כי

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

הנוסחה מכונה **הבינום של ניוטון**.

נשים לב שיש סימטריה במקדמי הבינום: $\binom{n}{k} = \binom{n}{n-k}$. יש למקדמים אלו כל מיני תכונות נחמדות אבל לא נתעכב על זה.

דוגמאות לשימוש בנוסחת הבינום של ניוטון

דוגמאות:

1. ניקח למשל $n=4$. נחשב את **מקדמי הבינום**:

$$\binom{4}{0}=\frac{4!}{0!4!}=1,\ \binom{4}{1}=\frac{4!}{1!3!}=4,\ \binom{4}{2}=\frac{4!}{2!2!}=6,\ \binom{4}{3}=\frac{4!}{3!1!}=4,\ \binom{4}{4}=\frac{4!}{4!0!}=1.$$

לכן

$$(a+b)^4=a^4+4a^3b+6a^2b^2+4ab^3+b^4.$$

למשל, אם נציב $a=b=1$ נקבל:

$$16=(1+1)^4=1+4+6+4+1.$$

2. זה קצת טריק, אבל בכל זאת מעניין:

$$\sum_{k=0}^{n}\binom{n}{k}=\sum_{k=0}^{n}\binom{n}{k}1^k\cdot 1^{n-k}=(1+1)^n=2^n.$$

2 שדות

2.1 הגדרה של שדה

שדות

קבוצות המספרים $\mathbb{Q}$ ו-$\mathbb{R}$ שונות מהאחרות $\mathbb{N},\mathbb{Z}$ במובן שניתן לחלק בכל מספר שונה מאפס. המספרים הממשיים והמספרים הרציונלים הם "מגרשי משחקים" של מספרים שמכונים **שדה**. הנה הגדרה מדויקת:

הגדרה 6. (שדה) **שדה** הוא קבוצה $\mathbb{F}$ יחד עם שתי פעולות: חיבור וכפל, שמקיימות את התנאים הבאים.

1. הפעולות הן פעולות בינאריות: חיבור מסומן על ידי $a+b$ כאשר a,b איברים של הקבוצה $\mathbb{F}$, והתוצאה של החיבור $a+b$ היא גם איבר בקבוצה $\mathbb{F}$. כנ"ל לגבי הכפל $a\cdot b$.
2. אסוציאטיביות בחיבור ובכפל: לכל $a,b,c\in\mathbb{F}$ (כלומר: a,b,c איברים בתוך הקבוצה $\mathbb{F}$) מתקיים

$$\begin{cases}a+(b+c)=(a+b)+c\\ a\cdot(b\cdot c)=(a\cdot b)\cdot c\end{cases}.$$

3. קומוטטיביות בחיבור ובכפל: לכל $a, b \in \mathbb{F}$,

$$\begin{cases} a+b=b+a \\ a \cdot b = b \cdot a \end{cases}.$$

4. אדיש חיבורי ואדיש כפלי: קיימים איברים שונים $0, 1 \in \mathbb{F}$ כך שלכל $a \in \mathbb{F}$ מתקיים

$$\begin{cases} a+0=a \\ a \cdot 1 = a \end{cases}.$$

5. איבר נגדי: לכל $a \in \mathbb{F}$ קיים איבר $b \in \mathbb{F}$ כך ש-$a+b=0$.
6. איבר הופכי: לכל $0 \neq a \in \mathbb{F}$ קיים איבר $b \in \mathbb{F}$ כך ש-$a \cdot b = 1$.
7. דיסטריבוטיביות: לכל $a, b, c \in \mathbb{F}$ מתקיים $a \cdot (b+c) = a \cdot b + a \cdot c$.

הערה: לפעמים אומרים במקום תכונה 1 כי $\mathbb{F}$ **סגור** לחיבור ולכפל. נשתמש במינוח כזה בהמשך בהקשרים מסוימים אך לצורך הגדרת שדה, זה לא לגמרי מתאים.

התכונות אולי נראות ברורות מאליהן, אבל נראה מיד שאפילו בתוך קבוצות של מספרים שאנחנו כבר מכירים, חלקן לא תמיד מתקיימות. ככל שתתקדמו, תזכו לראות דוגמאות נוספות של קבוצות ופעולות שבהן תכונות כאלו שאנחנו רגילים אליהן פתאום לא מתקיימות.

נדגיש כי $a+b$ וכן $a \cdot b$ לאו דווקא מתאימים לפעולות החיבור והכפל אליהן אנו רגילים. אפשר למשל להמציא פעולות חדשות בין מספרים שלמים, ולשאול אם תכונות השדה מתקיימות עבורן.

דוגמאות בסיסיות עבור ההגדרה של שדה

דוגמאות:

1. $\mathbb{N}$ אינו שדה, למשל כי אין אדיש חיבורי.
2. $\mathbb{Z}$ אינו שדה, למשל כי אין הופכי לכל איבר.
   לדוגמה, אין אף מספר שלם k שמקיים $2k = 1$.
   יש לשים לב שיש כאן שימוש בכך ש-1 הוא האדיש הכפלי. זה כמובן נכון ומסתדר עם הסימון המוכר, אבל על פניו אולי יש מספר אחר שיכול לשמש כאדיש כפלי ושעבורו יש הופכי לכל איבר. זה כמובן לא יתכן, וקל לבדוק במקרה של $\mathbb{Z}$ שאין אדיש כפלי אחר. באופן כללי, מיד נראה שאין אפשרות לשני אדישים חיבוריים או שני אדישים כפליים בשדה.
3. המספרים הרציונלים $\mathbb{Q}$ עם פעולות החיבור והכפל המוכרות, הוא שדה. האדיש החיבורי הוא 0 והאדיש הכפלי הוא 1.
   לכל איבר יש נגדי: $\frac{-m}{n}$.
   לכל איבר שונה מאפס יש הופכי: $\frac{n}{m}$.
   יש תכונות נוספות שצריך לבדוק כמובן. כל מה שמופיע בהגדרה.
4. המספרים הממשיים $\mathbb{R}$ עם פעולות החיבור והכפל המוכרות, הוא שדה. לא הגדרנו אותו במדויק ולכן לא נוכל להוכיח טענה זו במדויק.

בניית שדות

ננסה להמציא שדה $\mathbb{F}$ שיש בו בדיוק 2 איברים: $\mathbb{F} = \{a, b\}$.

לפי ההגדרה, בכל שדה חייבים להיות שני מספרים שונים, שאחד מהם אדיש לחיבור והשני אדיש לכפל. לכן אחד מבין a, b הוא אדיש לחיבור, והשני הוא אדיש לכפל. נניח למשל ש-a אדיש לחיבור ו-b אדיש לכפל.

נכין טבלאות חיבור וכפל, באופן שדרישות השדה מתקיימות.

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

חשבו מדוע כל תוצאה מוגדרת כך, ובדקו שכל אקסיומות השדה אכן מתקיימות.

נסו לעשות זאת עם $3, 4, 5, 6$ איברים. זה יכול להיות קצת ארוך, אבל התוצאות מעניינות.

תכונות בסיסיות בשדה

משפט 7. (תכונות בסיסיות בשדה) יהי $\mathbb{F}$ שדה. אז:

1. איבר ה-0 יחיד, ואיבר ה-1 יחיד (למשל, אם $a, b \in \mathbb{F}$ שניהם אדישים לחיבור אז $a = b$).
2. לכל $a \in \mathbb{F}$ קיים איבר נגדי **יחיד**, ולכל $0 \neq a \in \mathbb{F}$ קיים איבר הופכי יחיד.
   האיבר הנגדי מסומן $-a$, והאיבר ההופכי מסומן a^{-1}.
3. לכל $a \in \mathbb{F}$ מתקיים כי $-(-a) = a$ (הנגדי של הנגדי הוא האיבר עצמו).
4. לכל $0 \neq a \in \mathbb{F}$ מתקיים כי $(a^{-1})^{-1} = a$.
5. לכל $a \in \mathbb{F}$ מתקיים כי $a \cdot 0 = 0$.
6. אם $a, b \in \mathbb{F}$ מקיימים כי $a \cdot b = 0$ אז $a = 0$ או $b = 0$.

באופן כללי, שני איברים שונים מ-0 אשר מכפלתם שווה ל-0 מכונים **מחלקי אפס**. לכן התכונה האחרונה היא: בשדה אין מחלקי אפס.

לפעם הבאה

מומלץ לעשות חזרה קצרה על המושגים הבאים לפני שבוע הבא:

1. חילוק עם שארית של מספרים שלמים, והמושג "מחלק" (מהתיכון).
2. מספרים מרוכבים (למי שלמד את זה בעבר).
3. טריגונומטריה בסיסית ($\sin\theta, \cos\theta$).

> *Being artificial doesn't mean it isn't real—it only means it has a purpose.*
>
> Brandon Sanderson, Yumi and the Nightmare Painter